Finite Fields and Their Applications 24 (2013) 105–117

Contents lists available at SciVerse ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Generalized Maiorana–McFarland class and normality of p-ary bent functions

Ayça Çeşmelioğlu [a,*,1], Wilfried Meidl [b,2], Alexander Pott [a]

[a] Otto-von-Guericke-University, Faculty of Mathematics, 39106 Magdeburg, Germany
[b] Sabancı University, MDBF, Orhanlı, Tuzla, 34956 İstanbul, Turkey

ARTICLE INFO

Article history:
Received 5 March 2013
Accepted 12 June 2013
Available online 16 July 2013
Communicated by Gary McGuire

MSC:
11T06
06E30
11T71

Keywords:
Bent functions
Maiorana–McFarland class
Normality
Coulter–Matthews bent functions

ABSTRACT

A class of bent functions which contains bent functions with various properties like regular, weakly regular and not weakly regular bent functions in even and in odd dimension, is analyzed. It is shown that this class includes the Maiorana–McFarland class as a special case. Known classes and examples of bent functions in odd characteristic are examined for their relation to this class. In the second part, normality for bent functions in odd characteristic is analyzed. It turns out that differently to Boolean bent functions, many – also quadratic – bent functions in odd characteristic and even dimension are not normal. It is shown that regular Coulter–Matthews bent functions are normal.

1. Introduction

For a prime p, let f be a function from an n-dimensional vector space V_n over $\mathbb{F}_p$ to $\mathbb{F}_p$. The *Walsh transform* of f is then defined to be the complex valued function $\widehat{f}$ on V_n

$$\widehat{f}(b) = \sum_{x \in V_n} \epsilon_p^{f(x)-\langle b,x\rangle}$$

* Corresponding author.
E-mail addresses: cesmelio@ovgu.de (A. Çeşmelioğlu), wmeidl@sabanciuniv.edu (W. Meidl), alexander.pott@ovgu.de (A. Pott).

[1] The author is supported by Tübitak BİDEB 2219 Scholarship Programme.
[2] The author is supported by Tübitak Project No. 111T234.

1071-5797/$ – see front matter
http://dx.doi.org/10.1016/j.ffa.2013.06.001

where $\epsilon_p = e^{2\pi i/p}$ and $\langle b, x\rangle$ denotes a (nondegenerate) inner product on V_n. The classical frameworks are $V_n = \mathbb{F}_p^n$ and $\langle b, x\rangle$ is the conventional dot product denoted by "$\cdot$", and $V_n = \mathbb{F}_{p^n}$ and $\langle b, x\rangle = \mathrm{Tr}_n(bx)$, where $\mathrm{Tr}_n(z)$ denotes the absolute trace of $z \in \mathbb{F}_{p^n}$. In this article we will consider examples in both frameworks, but general definitions and results will be formulated in the framework of $V_n = \mathbb{F}_p^n$.

The function f is called a *bent function* if $|\widehat{f}(b)| = p^{n/2}$ for all $b \in \mathbb{F}_p^n$. If $|\widehat{f}(b)| \in \{0, p^{(n+1)/2}\}$ for all $b \in \mathbb{F}_p^n$, then we call f *near-bent* (for $p = 2$ the term *semi-bent* is common), and more generally f is called s-plateaued for an integer $0 \leqslant s \leqslant n$ if $|\widehat{f}(b)| \in \{0, p^{(n+s)/2}\}$ for all $b \in \mathbb{F}_p^n$. We remark that for $p = 2$ the Walsh transform yields an integer. Hence if f is s-plateaued, then n and s must have the same parity. In particular, binary bent functions only exist for n even. For odd p, bent functions exist for n even and for n odd.

For the Walsh coefficient $\widehat{f}(b)$ we always have (cf. [14])

$$p^{-n/2}\widehat{f}(b) = \begin{cases} \pm\epsilon_p^{f^*(b)}, & n \text{ even or } n \text{ odd and } p \equiv 1 \bmod 4, \\ \pm i\epsilon_p^{f^*(b)}, & n \text{ odd and } p \equiv 3 \bmod 4, \end{cases} \tag{1}$$

where f^* is a function from $\mathbb{F}_p^n$ to $\mathbb{F}_p$. A bent function $f : \mathbb{F}_p^n \to \mathbb{F}_p$ is called *regular* if for all $b \in \mathbb{F}_p^n$

$$p^{-n/2}\widehat{f}(b) = \epsilon_p^{f^*(b)}.$$

When $p = 2$, a bent function is trivially regular, and as can be seen from (1), for $p > 2$ a regular bent function can only exist for even n and for odd n when $p \equiv 1 \bmod 4$. A function $f : \mathbb{F}_p^n \to \mathbb{F}_p$ is called *weakly regular* if, for all $b \in \mathbb{F}_p^n$, we have

$$p^{-n/2}\widehat{f}(b) = \zeta\epsilon_p^{f^*(b)}$$

for some complex number ζ with $|\zeta| = 1$, otherwise it is called *not weakly regular*. By (1), ζ can only be ± 1 or $\pm i$. Note that regular implies weakly regular.

The classical example for a bent function is the *Maiorana–McFarland* bent function from $\mathbb{F}_p^m \times \mathbb{F}_p^m = \mathbb{F}_p^{2m}$ to $\mathbb{F}_p$ defined by

$$f(x, y) = x \cdot \pi(y) + \sigma(y)$$

for a permutation π of $\mathbb{F}_p^m$ and an arbitrary function $\sigma : \mathbb{F}_p^m \to \mathbb{F}_p$. We remark that the condition that π is a permutation is necessary and sufficient for f being bent. The Maiorana–McFarland function is always a regular bent function. Moreover $f(x, \pi^{-1}(0)) = \sigma(\pi^{-1}(0))$ is constant for all $x \in \mathbb{F}_p^m$, hence a Maiorana–McFarland function is an example of a normal function, which is defined as follows. For an even integer $n = 2m$, a function $f : \mathbb{F}_p^n \to \mathbb{F}_p$ is called *normal* if there is an affine subspace of dimension $m = n/2$ on which the function is constant, f is called *weakly normal* if there is an affine subspace of dimension $m = n/2$ on which the function is affine, see [17]. The notion of normal Boolean functions was introduced in [12]. By counting arguments one can show that nearly all Boolean functions are non-normal, however almost all known Boolean bent functions are normal, see [17].

2. A generalization of the Maiorana–McFarland class

Based on some earlier results on constructing Boolean bent functions from near-bent functions (see [10,17]), in [6] the following general idea for constructing bent functions has been suggested:

Let m and $1 \leqslant s \leqslant m$ be integers, and for each $u = (u_1, u_2, \ldots, u_s) \in \mathbb{F}_p^s$, let $f_u(x) : \mathbb{F}_p^m \to \mathbb{F}_p$ be an s-plateaued function. Let $supp(\widehat{f_u})$ denote the support of the Fourier transform of the function f_u, i.e. $supp(\widehat{f_u}) = \{b \in \mathbb{F}_p^m \mid \widehat{f_u}(b) \neq 0\}$. If $supp(\widehat{f_u}) \cap supp(\widehat{f_v}) = \emptyset$ for $u, v \in \mathbb{F}_p^s, u \neq v$, then the function $F(x, y)$ from $\mathbb{F}_p^m \times \mathbb{F}_p^s = \mathbb{F}_p^{m+s}$ to $\mathbb{F}_p$ defined by